PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-304206
(43)Date of publication of application : 13.11.1998

(51)Int.Cl. H04N 1/44
G09C 5/00
H04L 9/14
H04N 1/41
H04N 7/30
H04N 7/167

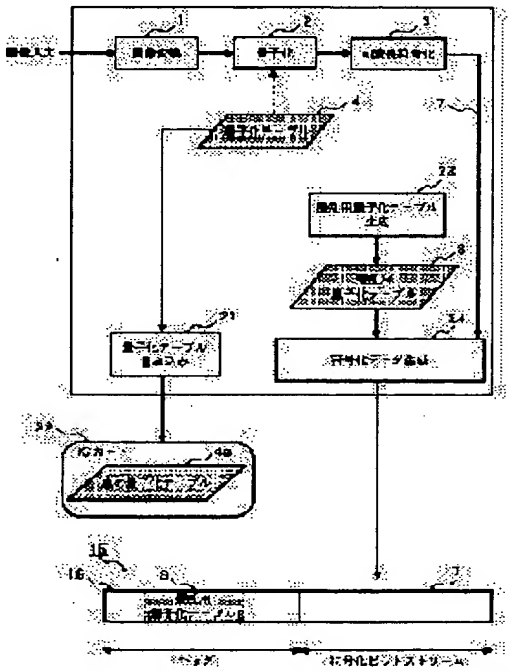
(21)Application number : 10-025706
(22)Date of filing : 06.02.1998

(71)Applicant : N T T DATA:KK
(72)Inventor : TOMURA MOTOHISA

(30)Priority
Priority number : 09 42005 Priority date : 26.02.1997 Priority country : JP

(54) IMAGE CODING/DECODING SYSTEM AND IMAGE CODING AND DECODING DEVICE FOR THE SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an image coding/decoding system in which the security of image data is improved while keeping the service performance for image data distribution.
SOLUTION: A scrambling quantization table 8 different from a quantization table 4 used for coding is described onto a header 16 of coded data 15 that are generated by image coding and the resulting coded data 15 are distributed to an opposite party. A copy 4a of the quantization table 4 in use is stored in an IC card 22 and the card is mailed to the opposite party. In the case of reproducing by the opposite party, the opposite party does not use the scrambling quantization table 8 but read the true quantization table 4a from the IC card 22 and decodes the coded data by using the table 4a. Since a party not receiving the IC card 22 decodes the coded data 15 by using the scrambling quantization table 8 included in the coded data 15, the party cannot normally reproduce the image. However, even in this case, a degree of scattering of the scrambling quantization table 8 is designed properly to allow even the party to grasp an outline of the image.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] In the method for receiving and decrypting the image data which transmitting-side equipment encodes image data and transmits and by which receiving-side equipment was encoded An image coding means by which said transmitting-side equipment encodes image data using a predetermined key, A different key for disturbance from the key which said image coding means used is added to the output data of said image coding means. A coded data generation means to generate the coded data which should be sent to said receiving-side equipment, A key acquisition means by which have a key preservation means to save the same true key as the key which said image coding means used to a predetermined key transfer medium, and said receiving-side equipment acquires a key from said key transfer medium, Image coding / decryption method characterized by having decrypted said coded data which received from said transmitting-side equipment using the key from said key acquisition means, and having an image decryption means to reproduce said image data.

[Claim 2] Image coding / decryption method characterized by setting to a method according to claim 1, having a quantization means by which said image coding means quantizes said image data using the predetermined quantization table as said predetermined key, and having a reverse quantization means by which said image decryption means reverse-quantizes said image data using the quantization table as a key from said key acquisition means.

[Claim 3] Image coding / decryption method characterized by equipping said receiving-side equipment with a key extract means to extract said key for disturbance from said coded data, further in the method of two claim 1 and given in any 1 term, and an image decryption means using alternatively the key from said key acquisition means, and said key for disturbance from said key extract means.

[Claim 4] It is image coding / decryption method characterized by for said image decryption means using the key from said key acquisition means in a method according to claim 3 when the key from said key acquisition means is supplied, and using said key for disturbance from said key extract means when the key from said key acquisition means is not supplied.

[Claim 5] Image coding / decryption method characterized by said key transfer medium being the data storage which can be conveyed in the method of two claim 1 and given in any 1 term.

[Claim 6] Image coding / decryption method characterized by being what currently can reproduce the image data by which disturbance was carried out to extent which can grasp the outline of the original image data in the method of two claim 1 and given in any 1 term when said key for disturbance decrypts said coded data using this.

[Claim 7] The image coding equipment characterized by to have an image coding means encode image data using a predetermined key in the equipment which encodes image data, a coded data generation means add a different key for disturbance from the key which said image coding means used to the output data of said image coding means, and generate coded data, and a key preservation means save the same true key as the key which said image coding means used to a predetermined key transfer medium.

[Claim 8] Image decryption equipment equipped with an image decryption means decrypt said coded data, using alternatively either of the internal keys from [from the coded data containing an internal key and the encoded image data] a key acquisition means acquire a predetermined key transfer medium to an external key in the equipment for decoding the original image data, and the external key and said key extract means from a key extract means extract an internal key from said coded data, and said key acquisition means.

[Claim 9] A different key for disturbance from the key which an image coding means to encode image data using a predetermined key, and said image coding means used is added to the output data of said image coding means. As image coding equipment equipped with a coded data generation means to generate coded data, and a key preservation means to save the same true key as the key which said image coding means used to a predetermined key transfer medium The record medium which supported the program as which a computer is operated and in which computer reading is possible.
[Claim 10] In the equipment for decoding the original image data from the coded data containing an internal key and the encoded image data From a key acquisition means to acquire an external key from a predetermined key transfer medium, and said coded data As image decryption equipment equipped with an image decryption means to decrypt said coded data, using alternatively either the external key from a key extract means to extract an internal key, and said key acquisition means, and the internal key from said key extract means The record medium which supported the program as which a computer is operated and in which computer reading is possible.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to image coding / decryption method for planning security of image data.
[0002]
[Description of the Prior Art] In the image coding method represented by JPEG etc., coding processing is conventionally performed by the flow shown in drawing 1 . That is, after changing an input image into the data of another dimension by the image transformation 1, such as DCT (discrete cosine transform), quantization 2 is performed and, finally variable length coding 3, such as Huffman coding, is given to quantization data.
[0003] Coded data 5 consists of a header 6 and a coding bit stream 7. As shown in drawing, the value of the quantization table 4 used for coding processing is included in the header 6 of coded data 5.
[0004] Drawing 2 shows the conventional image decryption method.
[0005] In decryption processing, after performing header analysis 11 of the coded data inputted and then performing the variable-length decryption 12, reverse quantization 13 is performed using the quantization table 4 obtained in the header analysis 11, finally inverse transformation 14 is performed, and it reproduces and outputs to the usual image data.
[0006] Moreover, in order to improve security nature, it may encipher to data, such as an image. In this case, as shown in drawing 3 , it is common to give encryption 15 to the whole data.
[0007]
[Problem(s) to be Solved by the Invention] In image coding / decryption method shown in drawing 1 and drawing 2 , since security is not given to an image, if the software equipped with the decode function of the same method etc. is used, an image is reproducible. Therefore, there is a problem that redistribution of the image by the non-authority person etc. cannot be prevented.
[0008] If the cipher system shown in drawing 3 is used, security nature will improve. However, since image data will be completely concealed by encryption, an image is unreproducible if there is no decryption software of the same method etc. Therefore, there is a problem that serviceability is missing.
[0009] Then, this invention aims at offering image coding / decryption method which can also aim at

improvement in security nature, maintaining the serviceability in image data distribution.
[0010]
[Means for Solving the Problem] It has a coded data generation means adds a different key for disturbance from the key which an image coding means to by_which the equipment of the side which transmits an image encodes image data by image coding / decryption method of this invention using a predetermined key, and an image coding means used to the output data of an image coding means, and generate the coded data which should transmit, and a key preservation means save the same true key as the key which an image coding means used to a predetermined key transfer medium. Moreover, the equipment of the side which receives coded data is equipped with a key acquisition means to acquire a key from a key transfer medium, and an image decryption means to decrypt the coded data which received from transmitting-side equipment using the key from a key acquisition means, and to reproduce image data.
[0011] According to the method of this invention, by sending the same true key as the key used by coding of an image to a receiving side through a key transfer medium, a true key can be acquired from the medium, coded data can be decrypted using this, and normal image data can be obtained by the receiving side. On the other hand, since the non-authority person to whom a key transfer medium is not supplied cannot but decrypt using the key for disturbance added to the coded data, he cannot get normal image data.
[0012] What is necessary is to be able to use for a key transfer medium the data storage in which conveyance like an IC card, a disk, or nonvolatile memory is possible, and just to distribute it to a receiving side. Or using a communication network as a key transfer medium, coded data is the different approach that security nature is high as much as possible or the different root, and a true key may be distributed to a receiving side.
[0013] Although the quantization table used for the quantization in the case of coding and the reverse quantization in the case of a decryption can be used as a key, it is not necessarily restricted to this. It seems that what is necessary is to be the data which cannot perform a normal decryption, a table, a parameter, or a file, and just to be able to make it secret for a third person if it is used in common by image coding and decryption in short and there is this [no].
[0014] However, even if there is no true quantization table, it can make it possible to see the outline of an image with common image reconstruction software etc. by setting up disturbance extent of a disturbance dosage child-ized table moderately, when a quantization table is used for a key. This approach is effective to show the outline of the some of an image in order to evoke attractiveness to consumers. In addition, although the image coding equipment of this invention and decryption equipment can be typically carried out by computer, the program for it can lead, and can install or load various media, such as disk mold storage, semiconductor memory, and a communication line, to a computer.
[0015]
[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained based on an accompanying drawing.
[0016] Drawing 4 shows 1 operation gestalt of the transmitting-side equipment according to this invention.
[0017] It prepares in a transmitting side, and like the conventional example shown in drawing 1 , after ****** image coding equipment 201 performs image transformation 1, such as DCT, to an input image using the predetermined quantization table 4 and changes it into the data of another dimension, it performs quantization 2 and, subsequently gives variable length coding 3, such as Huffman coding. And a header 16 is added to the coding bit stream 7 obtained by variable length coding 3, and the final coded data 15 is generated. At this time, this equipment 201 describes a quantization table 8 for a disturbance which is different in the quantization table 4 actually used for the header 16 of coded data 15 and which was prepared independently. And about the actually used quantization table 4, the copy (henceforth "true quantization table") 4a is saved at suitable storage. This true quantization table 4a is distributed to the just authority person who can receive service as a key for decoding an image correctly by root where coded data 15 is another. For example, although coded data 15 is distributed on-line through a network, true quantization table 4a is distributed with reliable off-line delivery means (for example, mailing etc.).
[0018] In addition, although generation of image transformation 1, quantization 2, variable length coding 3, and coded data 15 etc. can be carried out by the hardware of dedication, typically, it is carried out by activation of a computer program.
[0019] Drawing 5 shows 1 operation gestalt of the receiving-side equipment according to this invention.
[0020] The image decryption equipment 202 formed in the receiving side performs the header analysis 11, the variable-length decryption 12, the reverse quantization 13, and inverse transformation 14 to the inputted coded data 15 like the conventional example shown in drawing 2 . However, this equipment 202 can use now

alternatively the disturbance dosage child-ized table 8 extracted from the header 16 in the header analysis 11, and true quantization table 4a distributed by another root by the reverse quantization 13 by switch INGU 10. That is, in switching 10, if true quantization table 4a is supplied, this true quantization table 4a is chosen and true quantization table 4a is not supplied, the disturbance dosage child-ized table 8 obtained in the header analysis 11 is chosen.

[0021] A right image can be reproduced when true quantization table 4a is supplied to equipment 202. Since reverse quantization 13 will be performed on the other hand using the disturbance dosage child-ized table 8 when the case where true quantization table 4a is not supplied to equipment 202, the common image reconstruction software which does not have the function of switching 10, without using this equipment 202 are used, only the image by which disturbance was carried out is reproducible.

[0022] In addition, although the header analysis 11, the variable-length decryption 12, the reverse quantization 13, inverse transformation 14, and switching 10 can be carried out by the hardware of dedication, typically, they are carried out by activation of a computer program.

[0023] Hereafter, the above-mentioned operation gestalt is explained more concretely.

[0024] Drawing 6 shows the configuration of image coding equipment 201 more to a detail.

[0025] Image coding equipment 201 records true quantization table 4a on IC card 22 by performing the write-in process 21 while performing the coding processes 1, 2, and 3 as already explained. Moreover, the table generation process 23 generates the disturbance dosage child-ized table 8, and the disturbance dosage child-ized table 8 is recorded on the header 16 of coded data 15 according to the coded data generation process 24.

[0026] Drawing 7 shows the configuration of image decryption equipment more to a detail.

[0027] Image decryption equipment 202 will read true quantization table 4a from the IC card 22 according to the table reading process 31, if IC card 22 is set. And the switching process 10 makes automatic selection of the true quantization table 4a, and passes the reverse quantization process 13. On the other hand, if IC card 22 is not set, the switching process 10 chooses the disturbance dosage child-ized table 8 from the header analysis process 11, and passes it to the reverse quantization process 13.

[0028] According to the above-mentioned operation gestalt, security can also be raised, without spoiling the serviceability of image distribution greatly. Moreover, extent and mode which carry out disturbance of the image can be freely set up by the design of the disturbance dosage child-ized table 8. For example, you may enable it to grasp the outline of an image by moderate disturbance. Thereby, the effectiveness of making attractiveness to consumers evoke etc. can also be acquired.

[0029] In addition, this invention can be carried out not only with the above-mentioned operation gestalt but with other various gestalten. For example, the key of security reservation may be recorded not only on an IC card but on another means, and may be distributed.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the outline of the conventional image coding method.

[Drawing 2] It is the block diagram showing the outline of the conventional image decryption method.

[Drawing 3] It is the block diagram showing the conventional encryption processing.

[Drawing 4] It is the block diagram showing the outline of 1 operation gestalt of transmitting-side equipment of following this invention.

[Drawing 5] It is the block diagram showing the outline of 1 operation gestalt of receiving-side equipment of

following this invention.
[Drawing 6] It is the block diagram showing the detail of the image coding equipment of a transmitting side.
[Drawing 7] It is the block diagram showing the detail of the image decryption equipment of a receiving side.
[Description of Notations]
1 Image Transformation Process
2 Quantization Process
3 Variable-Length-Coding Process
4 Quantization Table
4a A true quantization table
8 Disturbance Dosage Child-ized Table
10 Switching Process
11 Header Analysis Process
12 Variable-length Decryption Process
13 Reverse Quantization Process
14 Inverse Transformation Process
15 Coded Data
16 Header
21 Table Write-in Process
22 IC Card
23 Table Generation Process
24 Coded Data Generation Process
31 Table Reading Process
201 Image Coding Equipment
202 Image Decryption Equipment

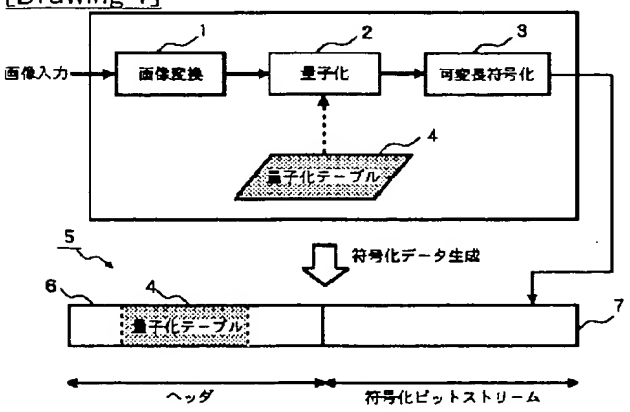
[Translation done.]

* NOTICES *

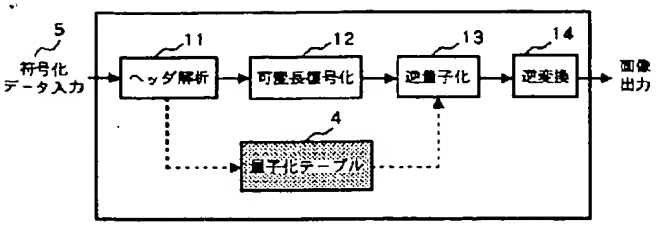
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

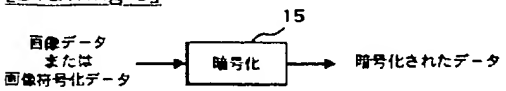
[Drawing 1]



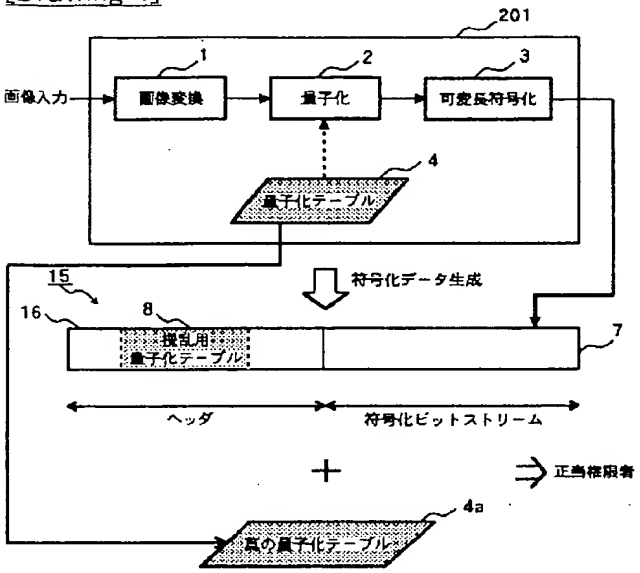
[Drawing 2]



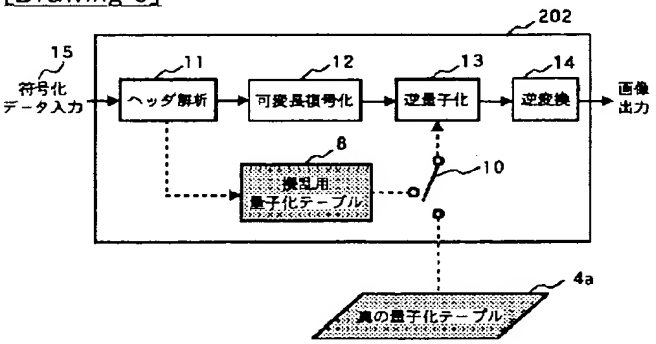
[Drawing 3]



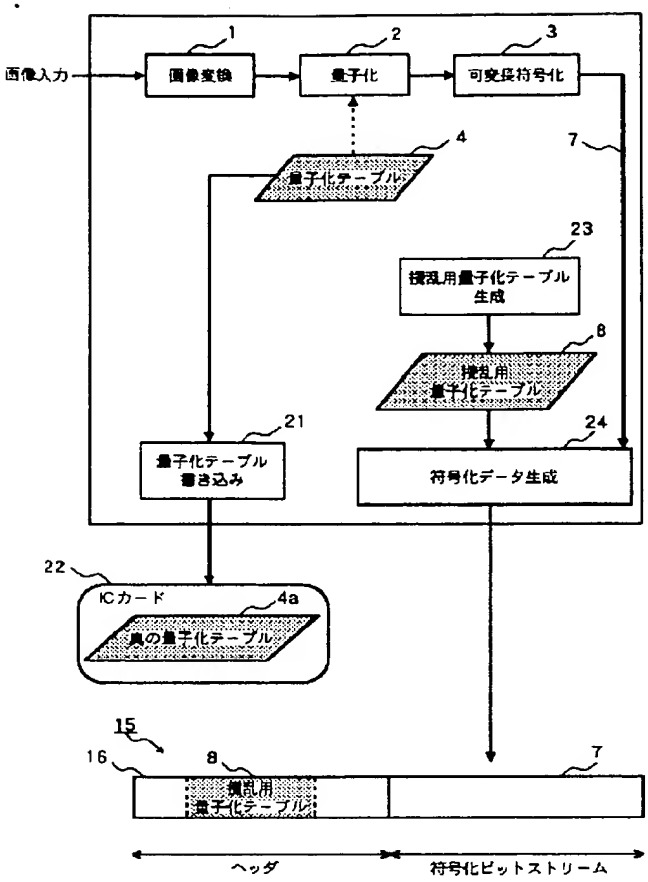
[Drawing 4]



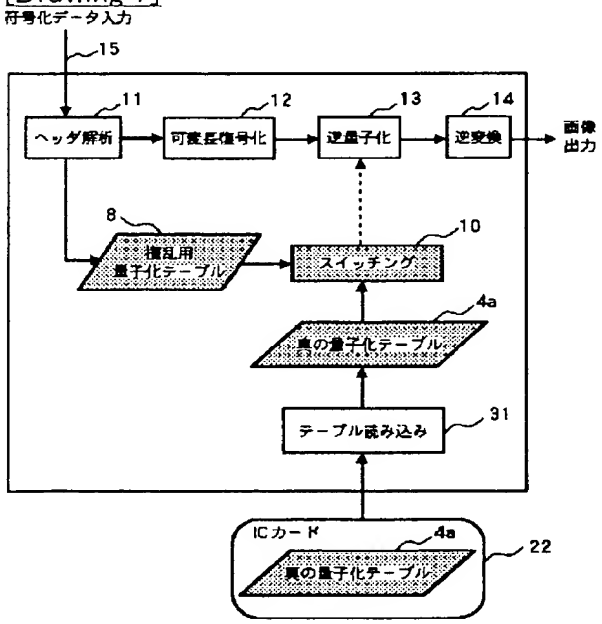
[Drawing 5]



[Drawing 6]



[Drawing 7]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－304206

(43)公開日　平成10年(1998)11月13日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｎ　1/44		Ｈ０４Ｎ	1/44	
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ	5/00	
Ｈ０４Ｌ　9/14		Ｈ０４Ｎ	1/41	Ｚ
Ｈ０４Ｎ　1/41		Ｈ０４Ｌ	9/00	６４１
7/30		Ｈ０４Ｎ	7/133	Ｚ

審査請求　未請求　請求項の数10　ＯＬ　（全 6 頁）　最終頁に続く

(21)出願番号　特願平10－25706

(22)出願日　平成10年(1998)２月６日

(31)優先権主張番号　特願平9－42005

(32)優先日　平９(1997)２月26日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号

(72)発明者　戸村　元久
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

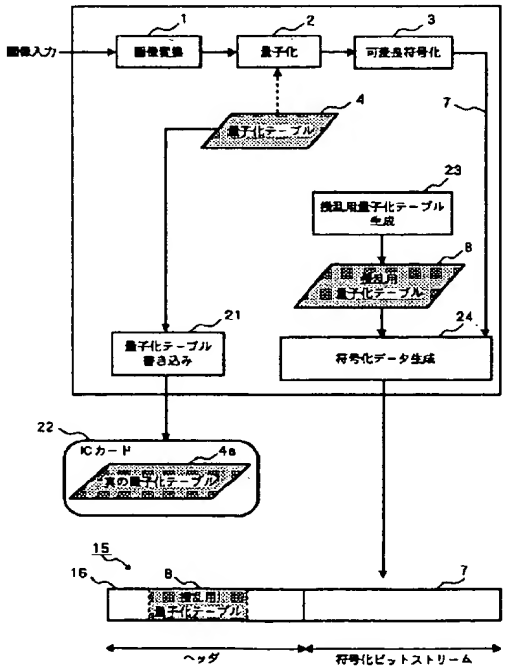
(74)代理人　弁理士　上村　輝之

(54)【発明の名称】　画像符号化／復号化方式及び同方式のための画像符号化及び復号化装置

(57)【要約】

【課題】　画像データ配布におけるサービス性を維持しつつ、セキュリティ性の向上も図ることができる画像符号化／復号化方式を提供する。

【解決手段】　画像符号化により生成した符号化データ１５のヘッダ１６に、符号化で使用した量子化テーブル４とは異なる撹乱用量子化テーブル８を記述して、その符号化データ１５を相手へ配信する。使用した量子化テーブル４のコピー４ａをＩＣカード２２に記憶させて、相手へ配送する。相手側では、画像を再生するとき、撹乱用量子化テーブル８を用いずに、ＩＣカード２２から真の量子化テーブル４ａを読み込み、これを用いて符号化データ１５を復号化する。ＩＣカード２２の配布を受けない者は、符号化データ１５に含まれる撹乱用量子化テーブル８を用いて、符号化データ１５を復号化することになるため、正常に画像が再生できない。しかし、この場合でも、撹乱用量子化テーブル８の撹乱程度を適度に設計しておくことにより、画像の概要は把握できるようにすることができる。



1

【特許請求の範囲】

【請求項１】　送信側装置が画像データを符号化して送信し、受信側装置が符号化された画像データを受信して復号化するための方式において、

前記送信側装置が、

所定のキーを用いて画像データを符号化する画像符号化手段と、

前記画像符号化手段が用いたキーとは異なる撹乱用キーを、前記画像符号化手段の出力データに付加して、前記受信側装置へ送られるべき符号化データを生成する符号化データ生成手段と、

前記画像符号化手段が用いたキーと同じ真のキーを所定のキー伝達媒体に保存するキー保存手段とを備え、

前記受信側装置が、

前記キー伝達媒体からキーを取得するキー取得手段と、

前記キー取得手段からのキーを用いて、前記送信側装置から受信した前記符号化データを復号化して、前記画像データを再生する画像復号化手段とを備えたことを特徴とする画像符号化／復号化方式。

【請求項２】　請求項１記載の方式において、

前記画像符号化手段が、前記所定のキーとしての所定の量子化テーブルを用いて、前記画像データを量子化する量子化手段を有し、

前記画像復号化手段が、前記キー取得手段からのキーとしての量子化テーブルを用いて、前記画像データを逆量子化する逆量子化手段を有することを特徴とする画像符号化／復号化方式。

【請求項３】　請求項１及び２のいずれか１項記載の方式において、

前記受信側装置が、前記符号化データから前記撹乱用キーを抽出するキー抽出手段をさらに備え、

画像復号化手段が、前記キー取得手段からのキーと、前記キー抽出手段からの前記撹乱用キーとを、選択的に使用することを特徴とする画像符号化／復号化方式。

【請求項４】　請求項３記載の方式において、

前記画像復号化手段が、前記キー取得手段からのキーが供給されているときは、前記キー取得手段からのキーを使用し、前記キー取得手段からのキーが供給されていないときは、前記キー抽出手段からの前記撹乱用キーを使用することを特徴とする画像符号化／復号化方式。

【請求項５】　請求項１及び２のいずれか１項記載の方式において、前記キー伝達媒体が、搬送可能なデータストレージであることを特徴とする画像符号化／復号化方式。

【請求項６】　請求項１及び２のいずれか１項記載の方式において、前記撹乱用キーが、これを用いて前記符号化データを復号化することにより、元の画像データの概略を把握できる程度に撹乱された画像データが再生できるようなものであることを特徴とする画像符号化／復号化方式。

2

【請求項７】　画像データを符号化する装置において所定のキーを用いて画像データを符号化する画像符号化手段と、

前記画像符号化手段が用いたキーとは異なる撹乱用キーを、前記画像符号化手段の出力データに付加して、符号化データを生成する符号化データ生成手段と、

前記画像符号化手段が用いたキーと同じ真のキーを所定のキー伝達媒体に保存するキー保存手段とを備えたことを特徴とする画像符号化装置。

【請求項８】　内部キーと符号化された画像データとを含む符号化データから元の画像データを復号するための装置において、

所定のキー伝達媒体から外部キーを取得するキー取得手段と、

前記符号化データから、内部キーを抽出するキー抽出手段と前記キー取得手段からの外部キー及び前記キー抽出手段からの内部キーのいずれかを選択的に用いて、前記符号化データを復号化する画像復号化手段とを備えた画像復号化装置。

【請求項９】　所定のキーを用いて画像データを符号化する画像符号化手段と、

前記画像符号化手段が用いたキーとは異なる撹乱用キーを、前記画像符号化手段の出力データに付加して、符号化データを生成する符号化データ生成手段と、

前記画像符号化手段が用いたキーと同じ真のキーを所定のキー伝達媒体に保存するキー保存手段とを備えた画像符号化装置として、コンピュータを機能させるプログラムを担持したコンピュータ読み取り可能な記録媒体。

【請求項１０】　内部キーと符号化された画像データとを含む符号化データから元の画像データを復号するための装置において、

所定のキー伝達媒体から外部キーを取得するキー取得手段と、

前記符号化データから、内部キーを抽出するキー抽出手段と前記キー取得手段からの外部キー及び前記キー抽出手段からの内部キーのいずれかを選択的に用いて、前記符号化データを復号化する画像復号化手段とを備えた画像復号化装置として、コンピュータを機能させるプログラムを担持したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、画像データのセキュリティを図るための画像符号化／復号化方式に関する。

【０００２】

【従来の技術】ＪＰＥＧ等に代表される画像符号化方式においては、従来、図１に示す流れで符号化処理が行われる。すなわち、入力画像をＤＣＴ（離散コサイン変換）等の画像変換１により別次元のデータに変換した後、量子化２を行い、最後に量子化データに対して、ハ

フマン符号化等の可変長符号化３を施す。

【０００３】符号化データ５はヘッダ６と符号化ビットストリーム７から構成される。符号化データ５のヘッダ６には、図に示すように、符号化処理に使用した量子化テーブル４の値が含まれる。

【０００４】図２は従来の画像復号化方式を示す。

【０００５】復号化処理においては、入力される符号化データのヘッダ解析１１を行い、次に可変長復号化１２を行った後、ヘッダ解析１１で得た量子化テーブル４を用いて逆量子化１３を行い、最後に逆変換１４を施して、通常の画像データに再生して出力する。

【０００６】また、セキュリティ性を向上するために、画像などのデータに対して暗号化を行う場合がある。この場合、図３に示すように、データ全体に対して暗号化１５を施すのが一般的である。

【０００７】

【発明が解決しようとする課題】図１、図２に示した画像符号化／復号化方式においては、画像にセキュリティが施されていないから、同じ方式の復号機能を備えたソフト等を用いれば、画像が再生できる。よって、無権限者による画像の再配布などを防ぐことができないという問題がある。

【０００８】図３に示す暗号化方式を用いれば、セキュリティ性は向上する。しかし、暗号化により画像データが完全に隠蔽されてしまうため、同じ方式の暗号解読ソフト等がないと画像が再生できない。よって、サービス性に欠けるという問題がある。

【０００９】そこで本発明は、画像データ配布におけるサービス性を維持しつつ、セキュリティ性の向上も図ることができる画像符号化／復号化方式を提供することを目的とする。

【００１０】

【課題を解決するための手段】本発明の画像符号化／復号化方式では、画像を送信する側の装置が、所定のキーを用いて画像データを符号化する画像符号化手段と、画像符号化手段が用いたキーとは異なる撹乱用キーを、画像符号化手段の出力データに付加して、送信すべき符号化データを生成する符号化データ生成手段と、画像符号化手段が用いたキーと同じ真のキーを所定のキー伝達媒体に保存するキー保存手段とを備える。また、符号化データを受信する側の装置が、キー伝達媒体からキーを取得するキー取得手段と、キー取得手段からのキーを用いて、送信側装置から受信した符号化データを復号化して画像データを再生する画像復号化手段とを備える。

【００１１】本発明の方式によれば、画像の符号化で使用したキーと同じ真のキーをキー伝達媒体を介して受信側に送付することにより、受信側では、その媒体から真のキーを取得して、これを用いて符号化データを復号化して正常な画像データを得ることができる。一方、キー伝達媒体が供給されない無権限者は、符号化データに付加された撹乱用キーを用いて復号化を行わざるを得ないため、正常な画像データを得ることができない。

【００１２】キー伝達媒体には、ＩＣカードやディスクや不揮発性メモリのような、搬送可能なデータストレージを用いることができ、それを受信側へ配布するようにすればよい。あるいは、通信ネットワークをキー伝達媒体として用いて、符号化データとは異なる、出来るだけセキュリティ性の高い方法又はルートで、真のキーを受信側へ配布してもよい。

【００１３】キーとしては、符号化の際の量子化及び復号化の際の逆量子化に用いる量子化テーブルが利用できるが、これに限られるわけではない。要するに、画像符号化と復号化で共通に用いられ、且つこれがないと正常な復号化ができないようなデータ、テーブル、パラメータ、又はファイルなどであって、第三者に秘密にしておくことができるようなものであればよい。

【００１４】しかし、量子化テーブルをキーに用いた場合には、撹乱用量子化テーブルの撹乱程度を適度に設定しておくことにより、真の量子化テーブルがなくても一般の画像再生ソフト等により画像の概要が見れるようにすることができる。この方法は、購買意欲を喚起するために画像の若干の概要を見せたい場合などに有効である。なお、本発明の画像符号化装置、復号化装置は典型的にはコンピュータによって実施することができるが、そのためのプログラムは、ディスク型ストレージ、半導体メモリ、通信回線などの種々の媒体を通じてコンピュータにインストール又はロードすることができる。

【００１５】

【発明の実施の形態】以下、本発明の実施の形態を添付図面に基づいて説明する。

【００１６】図４は本発明に従う送信側装置の一実施形態を示す。

【００１７】送信側に設けれらた画像符号化装置２０１は、図１に示す従来例と同様に、入力画像に対し、所定の量子化テーブル４を用いてＤＣＴ等の画像変換１を施して別次元のデータに変換した後、量子化２を行い、次いでハフマン符号化等の可変長符号化３を施す。そして、可変長符号化３で得られた符号化ビットストリーム７に、ヘッダ１６を付加して、最終的な符号化データ１５を生成する。このとき、この装置２０１は、符号化データ１５のヘッダ１６に、実際に使用した量子化テーブル４とは異なる、別に用意した、撹乱用の量子化テーブル８を記述する。そして、実際に使用した量子化テーブル４については、そのコピー（以下、「真の量子化テーブル」という）４ａを適当なストレージに保存する。この真の量子化テーブル４ａは、画像を正しく復号するためのキーとして、サービスを受け得る正当権限者等に、符号化データ１５とは別のルートで配布される。例えば、符号化データ１５はネットワークを通じてオンラインで配布されるが、真の量子化テーブル４ａは信頼性の

高いオフライン配送手段（例えば郵送など）で配布される。

【００１８】なお、画像変換１、量子化２、可変長符号化３、及び符号化データ１５の生成などは、専用のハードウェアで実施することができるが、典型的には、コンピュータプログラムの実行によって実施される。

【００１９】図５は本発明に従う受信側装置の一実施形態を示す。

【００２０】受信側に設けられた画像復号化装置２０２は、図２に示す従来例と同様に、入力した符号化データ１５に対し、ヘッダ解析１１、可変長復号化１２、逆量子化１３及び逆変換１４を施す。ただし、本装置２０２は、ヘッダ解析１１でヘッダ１６から抽出した撹乱用量子化テーブル８と、別ルートで配布された真の量子化テーブル４ａとを、スイッチイング１０によって選択的に、逆量子化１３で使用できるようになっている。すなわち、スイッチング１０では、真の量子化テーブル４ａが供給されていれば、この真の量子化テーブル４ａを選択し、真の量子化テーブル４ａが供給されていなければ、ヘッダ解析１１で得た撹乱用量子化テーブル８を選択する。

【００２１】真の量子化テーブル４ａが装置２０２に供給されている場合は、正しい画像を再生できる。一方、真の量子化テーブル４ａが装置２０２に供給されていない場合や、この装置２０２を使用せずに、スイッチング１０の機能がない一般の画像再生ソフト等を使用した場合は、撹乱用量子化テーブル８を用いて逆量子化１３を行うことになるため、撹乱された画像しか再生できない。

【００２２】なお、ヘッダ解析１１、可変長復号化１２、逆量子化１３、逆変換１４、及びスイッチング１０は、専用のハードウェアで実施することができるが、典型的には、コンピュータプログラムの実行によって実施される。

【００２３】以下、上記実施形態をより具体的に説明する。

【００２４】図６は画像符号化装置２０１の構成をより詳細に示す。

【００２５】画像符号化装置２０１は、既に説明した通りの符号化プロセス１、２、３を行うと共に、書き込みプロセス２１を行うことにより、真の量子化テーブル４ａをＩＣカード２２に記録する。また、テーブル生成プロセス２３により撹乱用量子化テーブル８を生成し、符号化データ生成プロセス２４により、符号化データ１５のヘッダ１６に撹乱用量子化テーブル８を記録する。

【００２６】図７は画像復号化装置の構成をより詳細に示す。

【００２７】画像復号化装置２０２は、ＩＣカード２２がセットされていれば、テーブル読み込みプロセス３１により、そのＩＣカード２２から真の量子化テーブル４ａを読み込む。そして、スイッチングプロセス１０が、真の量子化テーブル４ａを自動選択して逆量子化プロセス１３へ渡す。一方、ＩＣカード２２がセットされていなければ、スイッチングプロセス１０は、ヘッダ解析プロセス１１からの撹乱用量子化テーブル８を選択し、逆量子化プロセス１３へ渡す。

【００２８】上記実施形態によれば、画像配信のサービス性を大きく損なうことなく、セキュリティも向上させることができる。また、撹乱用量子化テーブル８の設計により、画像を撹乱する程度や態様を自由に設定することができる。例えば、適度な撹乱によって、画像の概要を把握できるようにしてもよい。それにより、購買意欲を喚起させるなどの効果を得ることも出来る。

【００２９】なお、本発明は上記の実施形態だけでなく他の種々の形態でも実施することができる。例えば、セキュリティ確保のキーは、ＩＣカードに限らず、別の手段に記録して配布してもよい。

【図面の簡単な説明】

【図１】従来の画像符号化方式の概略を示すブロック図である。

【図２】従来の画像復号化方式の概略を示すブロック図である。

【図３】従来の暗号化処理を示すブロック図である。

【図４】本発明に従う送信側装置の一実施形態の概略を示すブロック図である。

【図５】本発明に従う受信側装置の一実施形態の概略を示すブロック図である。

【図６】送信側の画像符号化装置の詳細を示すブロック図である。

【図７】受信側の画像復号化装置の詳細を示すブロック図である。

【符号の説明】

１　画像変換プロセス
２　量子化プロセス
３　可変長符号化プロセス
４　量子化テーブル
４ａ　真の量子化テーブル
８　撹乱用量子化テーブル
１０　スイッチングプロセス
１１　ヘッダ解析プロセス
１２　可変長復号化プロセス
１３　逆量子化プロセス
１４　逆変換プロセス
１５　符号化データ
１６　ヘッダ
２１　テーブル書き込みプロセス
２２　ＩＣカード
２３　テーブル生成プロセス
２４　符号化データ生成プロセス
３１　テーブル読み込みプロセス

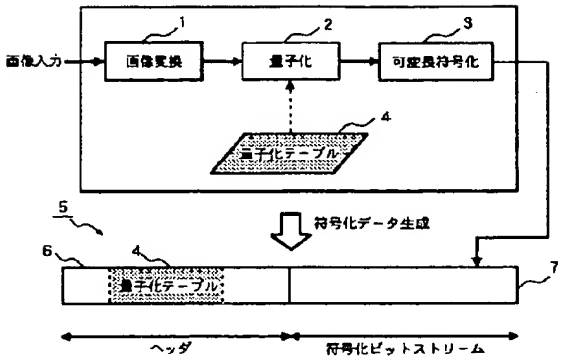
7

２０１　画像符号化装置

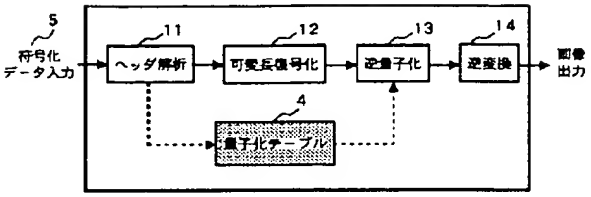
8

＊　＊２０２　画像復号化装置

【図１】

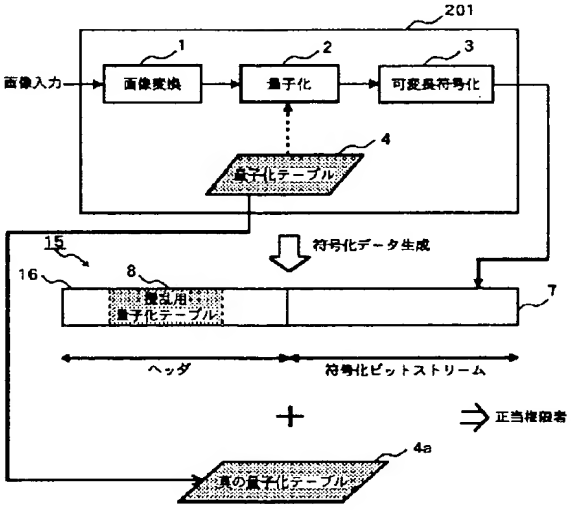


【図２】

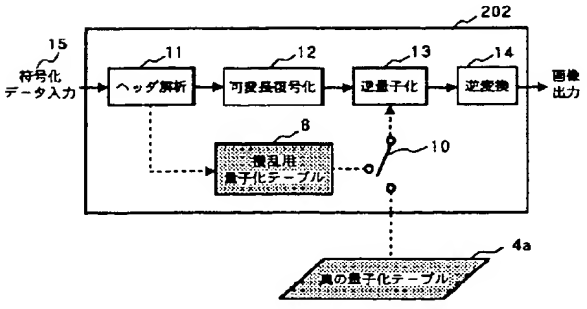


【図３】

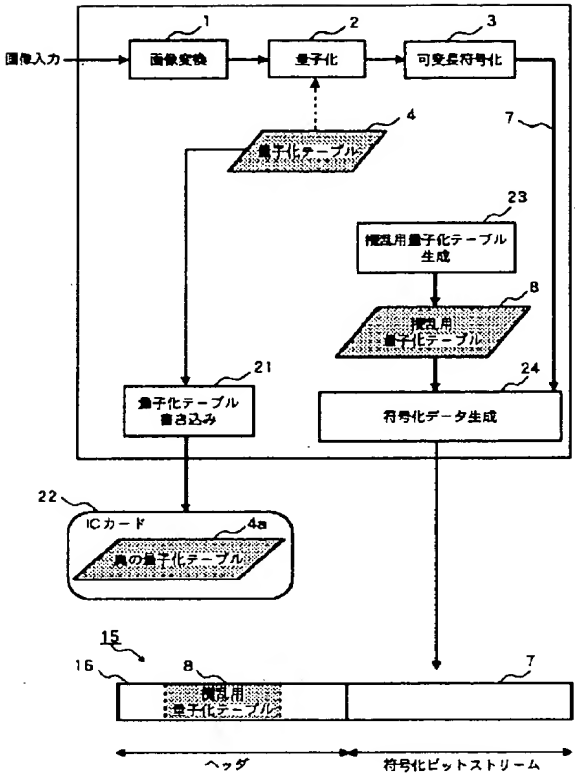
【図４】



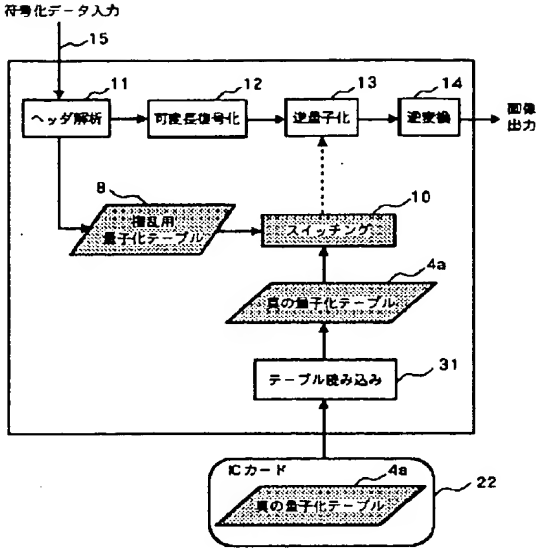
【図５】



【図６】



【図７】



フロントページの続き

(51)Int.Cl.⁶	識別記号	ＦＩ	
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	Ｚ